Maine State Government
Department of Administrative and Financial Services
Office of Information Technology (OIT)

Application Deployment Certification Policy

1.0 Purpose

1.1 Any computing application is subject to undergo a battery of tests to determine if it is suitable to be deployed into production. Based on the test results, the Chief Information Officer (CIO) makes the final determination whether the application should be placed into production.

1.2 As applications have become more complex, more interconnected, integrated with infrastructure and more exposed to the external world, it has become even more important to thoroughly vet them before they are deployed into production. This policy establishes a uniform and objective battery of tests that enables the CIO to evaluate the suitability of an application to be deployed into production.

2.0 **Definitions**

2.1 *State of Maine (SOM) Application:* A computer program, either specifically created or configured, to assist State of Maine users to perform a useful business function.

2.2 *Commodity Application:* Commercial-off-the-shelf (COTS) computer program, either consumed from the cloud or installed on a client device, that was not created or configured for any State of Maine-specific utility.

2.3 *Application Owners:* With respect to the application considered for deployment, the Executive Sponsor, Product Manager, and Product Owner are jointly and collectively identified as the Application Owners. If any of the roles is vacant, the same person fulfils more than one role, or there is a difference-in-opinion with respect to this Policy among the three roles, for this Policy, the decision of the Executive Director, Enterprise Shared Services, will be final and binding.

- 2.3.1 *Executive Sponsor* is the Agency Partner representative that has accountability for the strategic direction and budget of the program within the Agency that the application supports.
- 2.3.2 *Product Manager* is the OIT representative who works with the Agency Partner whose responsibilities include that the business objectives of an application are met.
- 2.3.3 *Product Owner* is the Agency Partner representative with the authority to

determine the business objectives of an application and the priority of the product features that are developed.

2.4 *Product Tester:* is one or more designee of the Product Manager and the Product Owner whose responsibilities include testing and validation of the performance, security, accessibility, and functionality of the application.

2.5 *Project Manager (PM):* is the DAFS representative whose responsibilities does not include certification of the deployment of the application. Their responsibilities are coordination and completion of application releases (including managing budget, scope, and schedule targets) when the Application Owners have mutually agreed upon the deliverables.

2.6 *Vendor Product Manager:* is the vendor representative for a purchased application, responsible for the product roadmap, release plan and application features. This may include Commercial off the Shelf (COTS), Software as a Service (SaaS), subscriptions, and other vendor managed and maintained technology solutions.

2.7 *Chief Information Security Officer (CISO):* is the State of Maine Chief Information Security Officer or designee.

2.8 *Recovery Point Objective (RPO):* The capability to restore data completely to its status at the time of the last valid backup, measured in hours. RPO limits how far to roll back in time and defines the maximum allowable data loss for the Application in the event of a catastrophic failure. It is determined collaboratively with the Product Owner.

2.9 *Recovery Time Objective (RTO):* The time it takes to recover the application, measured in hours. It defines the maximum downtime before there is significant business impact. RTO represents how long it takes to restore from the incident until normal operations are available. It is determined by the Product Owner.

2.10 *Broadband:* Is the transmission of wide bandwidth data over a high-speed internet connection. According to the Federal Communication Commission, (FCC) the definition of broadband internet is a minimum of 25 Mbps download and 3 Mbps upload speeds. Broadband provides high speed internet access via multiple types of technologies including fiber optics, wireless, cable, Digital Subscriber Line (DSL), and satellite.

2.11 *Support Model:* A collection of documented methods and resources used by the Application Owners to provide and manage end-to-end service and product delivery following deployment.

3.0 Applicability

This policy applies to all State of Maine applications being deployed under the purview of the CIO as defined in Statute[1]. This applies to deployment of new applications as well as modifications to existing applications, including but not limited

[1] https://legislature.maine.gov/statutes/5/title5ch163sec0.html

to infrastructure changes. This includes applications that are onsite or remotely hosted and internally or vendor managed. The OIT Governance framework for No Code-Low Code applications will apply to a selection of scalable and adaptive data management platforms. For No Code-Low Code applications, deployment certification applicability is limited to applications deemed critical to departmental operations or applications which transact in TLP:Red or TLP:Amber data classification.

4.0 Roles and Responsibilities

4.1 IT Directors: Enforce this Policy and determine applicability.

4.2 Application Owners: The Application Owners are responsible for ensuring appropriate tests are conducted, determining who should perform each test, and defining and documenting the support model. This certification consists of:

- 4.2.1 The names and signatures of the Product Manager, Product Owners, and the Executive Sponsor.
- 4.2.2 A summary result (Passed/Failed/Not Applicable) and a short paragraph clarifying that summary result, for each of the tests specified below, and the location of the test results.
- 4.2.3 An outline of the defined support model for the application.

4.3 Product Managers: The Product Managers are required to document applications into the Enterprise Application Inventory.

4.4 Testing

- 4.4.1 Any part of the testing required by this policy may be outsourced to a third-party without affecting the responsibility or the prerogative of the Application Owners. Irrespective of who executes a test, the Application Owners remain in charge of its execution. The Application Owners are not answerable to the third-party regarding the nature or the result of any outsourced test. Further, the third-party exclusively conveys the test results directly back to the Application Owners.
- 4.4.2 For OIT–Hosted applications, Application Owners will designate State personnel who will perform assigned applicable application tests.
- 4.4.3 For Remote-Hosted applications, it is a generally a combination of vetting vendor provided test results and State personnel performing applicable tests. If that vendor provided results for a specific application test are deemed acceptable by the Applications Director and subject matter experts (Chief Information Security Officer for Security, etc.), no further State personnel testing is required for that item. Should there be deficiencies, then additional testing must be conducted by either the vendor or by State personnel, until acceptable results are achieved.

4.5 Executive Director, Enterprise Shared Services: Owns and interprets this Policy.

4.6 Chief Information Officer (CIO): The CIO may delegate authority to certify or approve applications for deployment. Regardless of approving authority, certification of applications will be based on advice from any Director, and/or other subject matter experts.

4.7 OIT Accessibility Test Team: Interprets Accessibility Test results, reviews Voluntary Product Accessibility Templates (VPATs), and determines pass/fail results for Accessibility Test. Vendor provided test results may be accepted in lieu of OIT testing.

5.0 Directives

5.1 The following list defines the battery of application tests:

5.1.1 **User Acceptance Test:** Ensures functioning of all application features are fit for use.

5.1.2 **Accessibility Test:** Ensures compliance with the OIT accessibility policies and standards.

5.1.3 **Data Conversion and Migration Test:** Ensures the accurate migration of appropriate data.

5.1.4 **Interfaces Test:** Ensures proper functioning with all integrated or interrelated applications.

5.1.5 **Security Test:** Ensures the confidentiality, integrity, and availability of the application.

5.1.6 **Performance Test:** Ensures responsiveness under projected average and peak processing loads.

5.1.7 **Restoration Test:** Ensures full functioning of the application following an infrastructure rollback/restoration.

5.1.8 **Regression Test:** Applies exclusively to modifications of existing applications. Ensures that the new version does not compromise existing functionality.

5.1.9 **End-to End Test:** Ensures proper functioning of the application across all combinations of relevant hardware and software components. This may be inclusive of a Platform Test, as applicable.

5.2 General descriptions of the tests are provided below:

5.2.1 **User Acceptance Test:** An application must have complete, stable, and up-to-date documentation of the full set of its Use Cases in order to execute a User Acceptance Test. Use Case is defined as a sequence of steps between systems and users that accomplish a task and provide value for the user. Each Use Case must be executed individually and verified that it indeed delivers as expected. Beyond individual Use Cases, Application Owners must also know which Use Cases are likely to be invoked simultaneously with one another. All such likely combinations of Use Case interactions must be tested. Finally, it is also important to test a representative sample of actual end-users performing their daily jobs holistically, using the entirety of an application. At the completion of the User Acceptance Test, the Product Owner must confirm that the application meets all their expectations, or alternatively, that they are willing to accept any deficiencies.

5.2.2 **Accessibility Test:** The application must be tested to ensure its compliance with our Digital Accessibility Policy[2]. The accessibility team establishes the testing and assessment criteria and provides guidance. Testing may be conducted by our accessibility team, by the vendor, or by a vendor third-party. Vendor-provided test results must meet the requirements of the accessibility policy. Assessments of all test results are performed by the accessibility team.

5.2.3 **Data Conversion and Migration Test:** The record structures and formats of the legacy application may be modified as a result of the migration into the new application, or the data may have been migrated as is. In either case it must be ensured via testing that all business-critical data survived the conversion or migration. It is left to the Product Owner's discretion to determine exactly what constitutes 'business-critical data.'

5.2.4 **Interfaces Test:** An application must have complete and up-to-date documentation of all the data and workflow dependencies between itself and all applications it interacts with. All interactions must be tested. Interfaces must anticipate errors, and therefore, incorporate robust error-handling and error-logging capabilities. While it is desirable to exclusively utilize the Test environments of the various applications when testing the interfaces, it may be necessary under certain circumstances to pair the Test environment of this application with other environments of companion applications, as long as such other applications participate in the interface on a read-only basis. All Interfaces must be up to date in the Application Inventory system of record.

5.2.5 **Security Test:** The application must ensure the highest levels of Confidentiality (no unauthorized access), Integrity (delivered as planned; No unauthorized edits or tampering), and Availability (no denial-of-service). All personal, medical, and financial data, in motion, must be encrypted end-to-end, both inside and outside the State firewall. The encryption level is based on the data classification. Refer to the TLP (Traffic Light Protocol) in the OIT Data Classification Policy[3]. A full vulnerability assessment and penetration test must be performed on the application prior to certification. Tests may be executed by OIT's Information Security Office or acceptable tests may be provided by Cloud and vendor providers. Applications should guard against standard security vulnerabilities (Weak Credentials, Injection Attacks, Buffer Overflows, Cross-site Scripting, etc.), and be designed to thwart denial-of-service attacks. Beyond these generic requirements, an application may also need to satisfy additional specific, statutory requirements, as set forth by CJIS, HIPAA, FISMA/FIPS, SOX, GLBA, CROMERR, USA Patriot Act, FERPA, COPPA etc. All vulnerabilities must comply with the Vulnerability Scanning Procedure RA-5[4]. In all cases, regardless of classification level, the CISO has the final word regarding which vulnerabilities require remediation and which require a remediation plan/approved waiver prior to go-live.

[2] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DigitalAccessibilityPolicy.pdf
[3] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataClassificationPolicy.pdf
[4] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/VulnerablityScanningProcedure.pdf

5.2.6 **Performance Test:** Performance testing determines the responsiveness of the application to its users, and therefore, its acceptance and adoption. The application must meet customer requirements for response times under the projected average load and the expected peak load. The application must not cause unreasonable adverse impact on either network throughput or server loading. To safeguard against adverse user perception, the application must establish a two-tiered response time specification, one for data inquiry/lookup, and another for data modification transactions, for both Ethernet and broadband connectivity end-to-end. For performance testing, the application may consider using automated tools that simulate user behavior, including simultaneous and staggered loading. Beyond response times, other aberrations that must be investigated include non-linear performance, i.e., response time increasing disproportionately with loading, and response time varying during periods of constant load. This is a test that requires close cooperation with the SaaS provider and considers joint tenancy. Performance testing is preferably executed in an environment representative of the production environment, approved by the Application Owners.

5.2.7 **Restoration Test:** Subsequent to a point-in-time recovery of the entire suite of application components including but not limited to: the client-device, the webserver, the application server, the file server, and the database server, the application must be tested to ensure that it functions exactly as expected. The restoration test should encompass all components represented on the application's architecture diagram. This test demonstrates that in the event of a catastrophic failure, all system components ("all boxes") are recoverable. It is left to the Application Owners discretion to determine whether the entire suite of Use Cases or a core suite of essential Use Cases will be executed in the restoration test. Agreement is required between the infrastructure provider and the Application Owners on the two metrics of recovery: Recovery Point Objective, Recovery Time Objective and Acceptance Test Criteria.

5.2.8 **Regression Test**: This test applies whenever there is a modification to an existing application to ensure that the modification did not adversely affect existing functionality. A core suite of essential functions should be tested, irrespective of whether they underwent any modification as part of this deployment. It is left to the Product Owner's discretion to determine exactly what constitutes a 'core suite of essential functions.'

5.2.9 **End-to-End Test:** This test is to prove out the functionality in an environment that replicates the production environment. To replicate a production environment the application must be loaded and configured on all combinations of infrastructure and software that are planned for production. This may include hardware, operating systems, network configurations, segmentation, firewalls, and load balancers, etc., regardless of where the application resides, to verify that it works as expected from end-to-end. A platform test may be included in the scope of End-to-End Testing. It is left to the Application Owners discretion to determine exactly what constitutes an 'End-to-End' test.

5.3 Product Managers are responsible for ensuring appropriate documentation is maintained in the Applications Inventory.

6.0 Document Information

6.1 Initial Issue Date: September 22, 2010
6.2 Last Revision Date: December 1, 2023
6.3 Point of Contact: Policy Administrator, OIT, Enterprise.Architect@Maine.Gov
6.4 Approved By: Chief Information Officer, OIT
6.5 Legal Citation: Title 5, Chapter 163: Office of Information Technology[5]
6.6 Waiver Process: See the Waiver Policy[6]
6.7 Distribution: Internet[7]

[5] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[6] http://maine.gov/oit/policies/waiver.pdf
[7] https://www.maine.gov/oit/policies-standards